

## **REMARKS**

The Applicants respectfully request reconsideration in view of the amendments and the following remarks. Claims 1 and 14 are amended. Accordingly, claims 1-24 are pending in the application.

### **I. Claims Rejected Under 35 U.S.C. § 102**

Claim 1 rejected under 35 U.S.C. § 102(a) as being anticipated by Security Model and Authentication Protocol in EPON-based Optical Access Network, (hereinafter “Roh”) by Roh and Kim, published as part of Transport Optical Networks, 2003, Proceedings of the 2003 5<sup>th</sup> International Conference on 29 June-3, July 2003 (volume 1). To establish an anticipation rejection the Examiner must show that the cited reference teaches each element of a claim.

Claim 1, as amended, recites the following elements:

an optical line terminal for sending a discovery gate message to discover an optical network unit for data transmission, ***the discovery gate message including a public key of the optical line terminal***, and, if said optical network unit receives said discovery gate message and then requests data communication, sending an encrypted registration message including a permanent medium access control (MAC) address of said optical network unit to said optical network unit to notify said optical network unit that it has been registered and ***a general gate message encrypted by a session key, which is encrypted using said public key***, including said permanent MAC address of said optical network unit to said optical network unit to allocate a time slot to said optical network unit; and

said optical network unit for receiving said discovery gate message and then sending ***a registration request message, which is encrypted by the session key, including said session key encrypted by said public key*** to said optical line terminal to request the data communication therewith and ***a registration acknowledgement message encrypted by said session key*** to said optical line terminal to respond to said registration message.

(emphasis added). Roh fails to teach or suggest the above elements. In contrast, Roh relates to ONU authentication and the method to distribute a Session Key. First, Roh sends the GATE, REGISTER\_REQUEST and REGISTER messages for ONU Authentication in the *form of plaintext*. See Roh, Section 4.2. As a result, the security attacker can detect a traffic that is sent to each ONU, recognize a MAC address and a LLID of the ONU and analyze the characteristics of the Upstream traffic of the ONU such as quantity and form of the traffic of the ONU.

Therefore, Roh fails to teach the elements of “a general gate message encrypted by a session key, which is encrypted using said public key,” “a registration request message, which is encrypted by the session key, including said session key encrypted by said public key,” and “a registration acknowledgement message encrypted by said session key,” as recited in claim 1. In addition, as shown in Fig. 3, Roh must further send  $C_{olt}(K_{olt})$ , Timestamp messages to the ONU in the process of ONU authentication. This makes the ONU authentication process complicated and increases the amount of time spent processing the unnecessary traffic. Thus, in view of at least the foregoing reasons, Roh fails to teach each element of claim 1. Accordingly, reconsideration and withdrawal of the rejection of claim 1 are respectfully requested.

## **II. Claims Rejected Under 35 U.S.C. § 103**

Claims 2-24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Roh as applied to claim 1 above, and further in view of Cryptography and Network Security, by W. Stallings, 2<sup>nd</sup> Edition, 1999 (hereinafter “Stallings”).

In regard to dependent claims 2-13, these claims depend on base claim 1 and incorporate the limitations thereof. Therefore, for at least the reasons discussed in connection with claim 1, Roh fails to teach or suggest each element of claim 2-13. Further, Stallings fails to teach or suggest the missing elements. Instead, Stallings describes the method to implement the base algorithm in the field of cryptography and network security. However, the present invention is related to distributing, updating and restoring a Session Key in the structure of the EPON system as recited in claims 2-13. Therefore, Stallings fails to teach or suggest each of the elements in claims 2-13. Consequently, Roh in view of Stallings fails to teach or suggest each element of claims 2-13. Accordingly, reconsideration and withdrawal of the rejection of claims 2-13 are respectfully requested.

In regard to independent claim 14, this claim recites analogous limitations to those of claim 1. Therefore, for at least the reasons discussed in connection with claim 1, claim 14 is patentable over Roh. Further, the Applicants are unable to discern and the Examiner has not cited the portion of Stallings that teaches or suggests the missing elements of claim 14. Again, Stallings describes the method to implement the base algorithm in the field of cryptography and network security but fails to teach or suggest the elements related to distributing, updating and

restoring a Session Key in the structure of the EPON system in claim 14. Thus, for at least these reasons, Roh in view of Stallings fails to teach or suggest each element of claim 14. In addition, dependent claims 15-24 are patentable over Roh in view of Stallings because each of these claims depends on claim 14. Accordingly, reconsideration and withdrawal of the rejection of 14-24 are respectfully requested.

## **CONCLUSION**

In view of the foregoing, it is believed that all claims now pending patentably define the subject invention over the prior art of record, and are in condition for allowance and such action is earnestly solicited at the earliest possible date. If the Examiner believes that a telephone conference would be useful in moving the application forward to allowance, the Examiner is encouraged to contact the undersigned at (310) 207 3800.

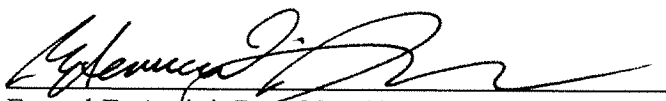
## **PETITION FOR EXTENSION OF TIME**

Per 37 C.F.R. 1.136(a) and in connection with the Final Office Action dated January 24, 2008, the Applicants respectfully petition the Commissioner for a one (1) month extension of time, extending the period for response to May 24, 2008. The Commissioner is hereby authorized to charge payment to Deposit Account No. 02-2666 in the amount of \$60.00 to cover the petition filing fee for a 37 C.F.R. 1.17(a)(1) small entity. A duplicate copy of this sheet is enclosed.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

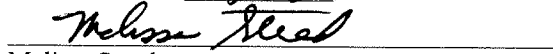
Dated: May 23, 2008

  
Farzad E. Amini, Reg. No. 42,261

1279 Oakmead Parkway  
Sunnyvale, CA 94085-4040  
(310) 207-3800

### **CERTIFICATE OF ELECTRONIC FILING**

I hereby certify that this paper is being transmitted online via EFS Web to the Patent and Trademark Office, Commissioner for Patents, Post Office Box 1450, Alexandria, Virginia 22313-1450, on 5-23, 2008.

  
Melissa Stead 5-23, 2008